

September 25, 2007

## Web-Address Theft Is Everyday Event

### Short or Memorable Domain Names Can Fetch Millions of Dollars

By KEVIN J. DELANEY  
September 25, 2007; Page B3

Like real-world theft, the hijacking of an Internet address can happen quickly and with little warning.

New York computer consultant Ronen Inowlocki knows firsthand. In July, a thief connived to take control of the yyy.com address that Mr. Inowlocki has owned for years. Mr. Inowlocki is still fighting to get it back, and can't access the "@yyy.com" email addresses he had used to communicate with clients. Meanwhile, the thief shifted the Internet address, also known as a domain, to a service in Germany and lists a mailing address in Iceland as his contact info.

Experts say the theft of Internet domain names occurs every day. The thieves -- taking advantage of companies that have either let down their guard or failed to take adequate precautions -- are often after financial gain, since short or memorable domains can be sold for millions of dollars and generate Web traffic and online-advertising revenue. Some domain hijackers are former employees or others looking to extract payments or take revenge.

"It's a complete rampage in our industry," says Monte Cahn, founder and chief executive of Moniker Online Services LLC in Pompano Beach, Fla., which handles domain services such as registrations and auctions.

Bob Parsons, chief executive officer of GoDaddy.com Inc., says the domain registrar is aware of daily hijacking incidents, with the frequency having increased as Internet use grows. But he and other domain experts say businesses can take simple measures to protect domains and notes there are techniques that help in the event they are hijacked.

Companies or individuals register Web domain names with some of the roughly 900 independent registrars worldwide or their affiliated resellers, usually paying a small annual fee. The registrars, who are accredited by the nonprofit Internet Corporation for Assigned Names and Numbers, collect identification and technical information from those registering.

That information is used to route Internet traffic so that when someone types a Web address, say, www.apple.com, into their browser software they are directed to Apple Inc.'s computer servers or when they send an email it ends up at the right place.

Once they register them, owners can transfer or sell the domains to other people. The sale of the "Porn.com" domain for \$9.5 million is the biggest reported sale so far this year, according to Domain Name Journal.

Internet domains are prized for several reasons, including their individuality, their brand recognition or simply because they are easy to remember, thus increasing customer traffic. Two companies can't both own and use "car.com" simultaneously, for example.

Numerous businesses have suffered from domain-name hijacking. In January 2005, a thief took control of "panix.com" away from Internet service provider Public Access Networks Corp. Emails to Panix customers bounced during the roughly two days that Panix lost control of the domain. In another case, it took the owner of "Sex.com" years to regain the domain after it had been hijacked using a forged letter to the registrar.

Domain experts say protecting the email address used to register the domain safe from break-ins is one of the most important steps to guarding the domain. Contact information for the person registering each domain is made publicly available online in a "Whois" database.

Hijackers sometimes break into the email address listed for a domain and use that account to change the domain owner's password with the registrar and authorize the domain's transfer. That's what happened to Mr. Inowlocki, with the domain thief breaking into his free **Yahoo** Inc. email account to seize yyy.com.

The domain experts say it is generally safer to use a corporate email address rather than a free Web email account offered by portals such as Yahoo. That's partly because the free Web email addresses can expire if they aren't used for a few years and then a domain hijacker can easily snatch them up. Passwords that are hard to guess and changed frequently are also key.

Owners need to "treat access to their email account as securely as they would treat credit-card numbers and other important information," says John Berryhill, a lawyer in Media, Pa., who handles domain-related issues.

Other measures to protect domains include keeping the information in the Whois database up to date, and registering it in the name of one of the owners or senior executives of a business. If the contact information held by the registrar isn't accurate, registrars can have a tougher time verifying who is trying to make any changes.

Domain experts say problems frequently occur when an outside contractor or employee registers a company's domain in their own name. Later on, they can use that to claim personal ownership of the domain in order to try to extract money from the business or cause problems.

Experts are divided on whether businesses should use private registration services, where registrars' information is listed in the Whois database rather than that of the owners. Such a measure could make it harder to impersonate the owner or crack into the email account. But Richard Lau, a London-based domain-name consultant, says that can make it harder for individuals trying to quickly verify ownership of a domain that has been transferred.

Mr. Lau advises businesses with valuable domains to use free and inexpensive services offered by some registrars that require additional layers of verification before a domain can be transferred from its owner. One of his clients has an "executive lock," which requires the company's chief executive to meet personally with the registrar's staff before it will transfer a domain. "The more valuable your domain name, the more you need to sacrifice convenience for security," says Mr. Lau.

Moniker, for one, offers a free executive-lock service as part of its domain registration service, which costs about \$8 to \$10 per year. Owners get a separate password they need to provide for the domain to be transferred. For a few dollars annually, GoDaddy.com will lock a domain from being transferred under most circumstances and extend the ownership for another year even if the owner forgets to renew it. At least one company offers insurance against domain theft.

When a domain is stolen, the owner needs to contact his registrar as soon as he becomes aware of it. In some cases, the owner's registrar can negotiate with the hijacker's registrar to have the domain returned. In others, the owner's registrar needs to file a formal complaint.

If those don't work, the owner can file a lawsuit. Mr. Lau says it is important to act quickly. "If the current owner sells the domain to an innocent third party, then it really gets murky and that's when you really have to be committed to a long fight," he says.

In Mr. Inowlocki's case, his registrar says it hasn't had any luck recovering the domain from the registrar that yyy.com was transferred to -- Key-Systems GmbH in Germany. Key-Systems CEO Alexander Siffrin says that is because Mr. Inowlocki's registrar, TierraNet Inc. unit DomainDiscover, hasn't yet made a formal complaint or gotten a court order.


Once it supplies "definite evidence of illegal activities involved in the transfer process, we will agree to transfer the domain name back," says Mr. Siffrin.

Write to Kevin J. Delaney at [kevin.delaney@wsj.com](mailto:kevin.delaney@wsj.com)<sup>1</sup>

URL for this article:  
<http://online.wsj.com/article/SB119068079815138145.html>

Hyperlinks in this Article:  
(1) <mailto:kevin.delaney@wsj.com>

#### DOW JONES REPRINTS

 This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit: [www.djreprints.com](http://www.djreprints.com).

- [See a sample reprint in PDF format.](#)
- [Order a reprint of this article now.](#)